The following document is intended for use by NRENs seeking to use, or actively using, the 2020 IaaS+ Framework.

The information contained in this document is intended as guidance but does not constitute legal advice.
MAP YOUR DATA TRANSFER
Do you process\(^1\) personal data?\(^2\)

Yes

IDENTIFY PLATFORM\(^3\)
Is platform operated by entity within EU/EEA location?

No

TRANSFER LOCATION
Is there a transfer outside EU/EEA? See link.

Yes

View list of countries where adequacy decisions apply See link.

No

ADEQUACY DECISION\(^4\)
Is there an adequacy decision?

Yes

Select the relevant platform provider in country

No

ASSESS LAWS
Conduct transfer impact assessment\(^5\)

How likely are the laws to be exercised in practice in relation to the data transfer?\(^7\)

Unlikely

Eliminate provider from candidate list

Likely
Data Transfer Checklist

Some, or all, of the below steps apply to all platforms regardless of where the platform resides

Know your Transfers
- Know what personal data is being processed

Verify platform
- Verify the platform relies on, Standard Contractual Clause (SCC), equivalence in law, Binding Corporate Rules (BCR). See Definitions

Assess laws of platform country
- Assess if laws infringe on specific safeguards of platform

Identify and adopt extra measures
- Measures to bring level of data protection to EU levels

Take any formal procedural steps
- Consult Data Protection Authority depending on platform

Re-evaluate level of protection
- Regularly monitor your levels of protection

Data Encryption Options

Below are some considerations in relation to data encryption and how it may impact on use of cloud services.

Encryption in Transit
- Data transferred over the public Internet can be encrypted using the TLS protocol or similar.

Encryption at Rest
- Data stored at rest, such as databases, object storage, files, etc., should be encrypted using available tools.
Transfer Impact Assessment (TIA)

**THE DATA**

- What personal data is being transferred?
- How sensitive is the data being transferred?
- How much is in the public domain?
- Where did the personal data originate from?

**THE LAWS**

- What technical measures are used to protect the data?
- What national laws apply in the jurisdiction?
- How are the laws exercised in practice?

**THE RESULT OF THE TIA**

- How likely are they to be exercised in relation to the platform?
Definitions

1. **Process(ing)** – any operation or set of operations performed on personal data.
2. **Personal data** – any information which is related to an identified or identifiable natural person.
3. **Platform** – some documentation may refer to Transfer Tool. In this instance this is the platform.
4. **Adequacy decision**
   There is an adequacy decision for countries like the UK, Switzerland, Argentina, Japan, etc. More information and the full list of countries can be found [here](#).
5. **Transfer impact assessment (TIA)**
   - Questionnaire to be completed by either party to the data transfer i.e. data importer or data exporter.
   - Clarifies organisation’s risks for transferring EU residents’ data to countries without adequacy under GDPR.
   - The TIA will be executed together with the Standard Contractual Clauses. Further information can be found [here](#).
6. For FISA, or similar, check if the perceived risk is higher than the threat of data theft by a malicious actor, including state sponsored data theft. If so consider:
   a) applying your existing risk mitigation strategies to protect against data theft and/or,
   b) bring Your Own Encryption Key and/or,
   c) if Binding Corporate Rules and Standard Contractual Clauses mitigate the perceived risk and/or,
   d) if there are improvements in the platform coming that can further reduce perceived risk
7. For more information on Binding Corporate Rules BCR click [here](#).